UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/315,628	05/20/1999	BJORN MARKUS JAKOBSSON	15	6758

7590 01/15/2004

RYAN & MASON LLP
90 FOREST AVENUE
LOCUST VALLEY, NY 11560

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 01/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/315,628	JAKOBSSON, BJORN MARKUS	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 May 1999*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) ~~*1-22 and 25-27*~~ 1-27 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *23 and 24* is/are allowed.

6)☒ Claim(s) *1-3,6,11-13,16,20-22 and 25-27* is/are rejected.

7)☒ Claim(s) *4,5,7-10,14,15 and 17-19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 May 1999* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

NORMAN M. WRIGHT 12/01
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2*.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-22 & 25-27 are pending.

2. The IDS of 3/10/2000 has been received and considered.

Drawings

3. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the process steps of claims 8, 18, 23 & 24 (key transformation) must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1, 2, 6, 11, 12, 16, 22, 25, 26 & 27 are rejected under 35 U.S.C. 102(b) as being anticipated by "Disavowal protocol for Chaum-van Antwerpen undeniable signature scheme" described in Handbook of Applied Cryptography by Menezes.

Regarding claims 1, 11, 22, 25, 26 & 27, Menezes discloses generating a signal/ w' and w (see page 477, steps 3 & 6) corresponding to information representative of first (see page 477, steps 1-7) and second (see page 477, step 8) proofs based on an operation associated with a cryptographic protocol (see page 476, Algorithm 11.122) wherein the first proof (see page 477, steps 1-7) is a proof that the operation/Algorithm 11.122 (see page 476) has been correctly performed, and the second proof (see page 477, step 8) is a proof that the first proof was correctly performed. The proof information signal/ w' and w is transmitted from the prover to the verifier (see page 477, steps 3 & 6) such that the verifier can determine if the operation associated with the cryptographic protocol is valid based on the proof information signal (see page 477, step 8).

Regarding claims 2 & 12, Menezes discloses a cryptographic protocol using an exponentiation operation (see page 477, step 2) and the proof information signal is based on a randomized instance of the exponentiation operation (see page 477, steps 2 & 3).

Regarding claims 6 & 16, Menezes discloses generating an indication that the prover is cheating if the second proof is not acceptable to the verifier (see page 477, step 8).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 3 & 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes. Menezes, in describing the disavowal protocol, lacks disclosure of a blind proof. However, Menezes teaches that blind signature schemes prevent the signer from observing the message it signs (see page 475, § 11.8.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to make the Menezes signature, as described above, a blind signature to gain the benefit of preventing the signer from observing the message it signs, as taught by Menezes (see page 475, § 11.8.1). One of ordinary skill in the art would have been motivated to perform such a modification to prevent the signer from observing the message it signs.

8. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes in view of "Distributed Provers with Applications to Undeniable Signatures" by Pedersen. Menezes, as described above, lacks the prover being a distributed prover. However, Pedersen teaches that using a distributed prover allows verification by others if the signer is unable to perform required duties without the signer having to give away the secret (see page 228, § 5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a distributed prover to allow verification by others without the signer having to give away the secret, as taught by Pedersen (see page 228, § 5). One of ordinary skill in the art would have been motivated to perform such a modification to allow verification by other than the signer without the signer having to give away the secret.

9. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes in view of Pedersen, in further view of Computer Architecture: A Quantitative Approach, Second Edition by Patterson and Hennessey. Menezes, as described above, lacks the prover being a distributed prover. However, Pedersen teaches that using a distributed prover allows verification by others if the signer is unable to perform required duties without the signer having to give away the secret (see page 228, § 5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a distributed prover to allow verification by others without the signer having to give away the secret, as taught by Pedersen (see page 228, § 5). One of ordinary skill in the art would have been motivated to perform such a modification to allow verification by other than the signer without the signer having to give away the secret. Menezes, as modified, still lacks a distributed processor. However, Patterson and Hennessey teach that using multiple processors increases performance and improves availability (see p. 636) and are used in distributed, networked environments (see p. 639). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to distribute processors amongst different machines to gain the benefits of increased performance and improved availability, as taught by Patterson and Hennessey (see pp. 636-639). One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefits of increased performance and improved availability.

Allowable Subject Matter

10. Claims 23 & 24 allowed.

11. Claims 2-10 & 12-21 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

12. The following is a statement of reasons for the indication of allowable subject matter:

Regarding claims 8, 18, 23 & 24, the prior art teaches, as stated by the applicant of the present invention (page 1 of specifications), taking an input of (g, y, m, s) for which $\log_g y = \log_m s$, however, the prior art relied upon fails to teach applying a key transformation protocol that produces a pair (G, Y) wherein G is a generator and Y is a public key, such that $X = \log_G Y$ can only be computed if $\log_g y = \log_m s$.

Regarding claims 4, 5, 14 & 15, the prior art relied upon fails to teach generating an indication that the operation was correctly performed if the first and second proofs are acceptable to the verifier. Further, the prior art relied upon fails to teach a step of generating an indication that the operation was not correctly performed if the first proof is not acceptable to the verifier but the second proof is acceptable to the verifier.

Regarding claims 7 & 17, the prior art relied upon fails to teach the steps set for in claims 7 & 17.

Regarding claims 9 & 19, the prior art relied upon fails to teach a key transformation protocol taking an input of the form (g, y, m, s, x) for which $\log_g y = \log_m s = x$ and generating a triple (G, Y, X) wherein X is a secret key, such that $Y = G^X$.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:30 p.m.. The examiner can also be reached on alternate Fridays from 8:00 a.m. – 4:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

MJS
11 December 2003

NORMAN M. WRIGHT
PRIMARY EXAMINER